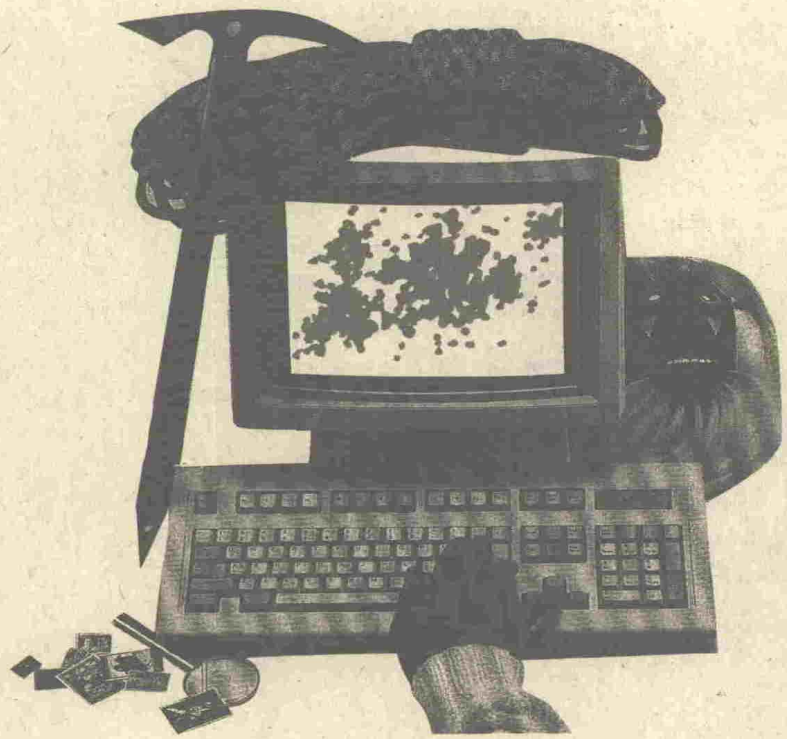
เอนก ศิรจริยาภิวัฒน์

หนทางต่อสู้และป้องกันไวรัสด้วย IMAGE และ UNFORMAT

ป้องกันฝันร้ายของข้อมูล ด้วยคำสั่งบางตัวในนอร์ตัน ยูทิลิตี้ เพื่อป้องกันไวรัสและ ให้ปราศจากความเสียหายที่เกิดขึ้น



ตามที่เราทราบกันอยู่แล้วว่า ไวรัสคอมพิวเตอร์บางประเภท ทำลายข้อมูลขั้นรุนแรงนั้นคือ ฟอร์แมตฮาร์ดดิสก์ ถ้าเราไม่เตรียมการป้องกันไว้ก่อน แม้เราพยายามกู้ข้อมูลนับพันครั้ง เราก็อาจไม่สามารถนำข้อมูลเหล่านั้นกลับมาได้ แต่ถ้าเราเตรียมการป้องกันไว้ก่อน การกู้ข้อมูลครั้งเดียวก็สามารถที่จะนำข้อมูลทั้งหมดกลับมาได้ แล้วเราจะไม่เตรียมการล่วงหน้าไว้ก่อนเชียวหรือครับ

อิมเมจ (IMAGE)

พอได้ยินคำนี้แล้วก็นึกถึงคำว่า IMAGINE ซึ่งหมายถึง ความฝัน, จินตนาการ แต่คำว่า อิมเมจในนอร์ตันยูทิลิตี้ หมายถึง โปรแกรมที่ใช้เก็บข้อมูลส่วนสำคัญของดิสก์ ซึ่งได้แก่บูตเรคอร์ด, FAT และไดเรคทอรี ไว้ในไฟล์ชื่อ IMAGE.DAT ซึ่งเมื่อมีอุบัติเหตุหรือข้อมูลถูกทำลายโดยการฟอร์แมตฮาร์ดดิสก์เราสามารถนำ IMAGE.DAT มากู้ข้อมูลได้ ไฟล์ IMAGE.DAT จะถูกสร้างเมื่อเราใช้โปรแกรม SFORMAT (ในฉบับหน้าเราจะมาศึกษาโปรแกรมตัวนี้), speed disk และโดยโปรแกรมอิมเมจ

การเก็บข้อมูลของบูตเรคอร์ด, FAT และไดเรคทอรี เราจะใช้โปรแกรมอิมเมจเป็นหลัก การใช้โปรแกรมอิมเมจทำได้โดยการพิมพ์คำว่า IMAGE เท่านั้น เมื่อสั่ง IMAGE ก็จะมีข้อความว่า updating IMAGE for drive X: เมื่อโปรแกรม IMAGE ทำงานเรียบร้อยก็จะมีข้อความ Finished updating IMAGE for drive X: (X หมายถึงไดรฟ์ที่ทำอิมเมจ) เราจะสังเกตว่า การใช้อิมเมจนั้นง่ายมาก เพราะฉะนั้นทุกครั้งก่อนปิดเครื่องควรจะสั่ง IMAGE (ในคู่มือของนอร์ตันจะแนะนำให้ใช้คำสั่งอิมเมจ ใน AUTOEXEC.BAT แต่ผมขอเพิ่มเป็นก่อนปิดเครื่อง เพราะว่าถ้าทำอิมเมจที่ AUTOEXEC.BAT เพียงอย่างเดียวจะทำให้ข้อมูลต่าง ๆ ที่เราทำงานหลังเปิดเครื่องจะไม่ได้รับการทำอิมเมจไว้ ทางที่ดีก่อนการปิดเครื่องควรจะสั่ง OFF โดยโปรแกรม OFF.BAT จะมีข้อมูลดังนี้

```
IMAGE C: เก็บข้อมูลส่วนสำคัญของฮาร์ดดิสก์
DISKMON/PARK ทำการพักหัวอ่าน/เขียนฮาร์ดดิส
```

ถ้าฮาร์ดดิสก์เรามีไดรฟ์อื่นด้วย เราก็เพิ่มข้อมูลของไดรฟ์นั้นใน OFF.

BAT ด้วย เช่น ถ้าเรามีไดรฟ์ D: โปรแกรม OFF.BAT ก็จะกลายเป็น

```
IMAGE C:
IMAGE D:
DISKMON/PARK
```

หมายเหตุ

ถ้าเครื่องของเรามี FRECOVER.DAT (เกิดจากการใช้นอร์ตันยูทิลิตี้ 4.5) เมื่อเราใช้อิมเมจ ไฟล์ FRECOVER.DAT จะถูกเปลี่ยนชื่อ (และเก็บข้อมูลใหม่) เป็น IMAGE.DAT

UNFORMAT

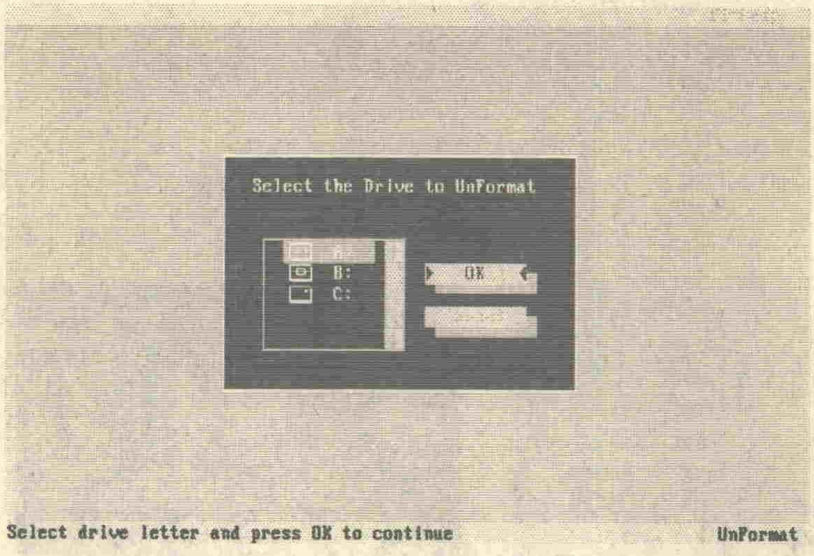
เมื่อถึงคราวจำเป็นที่จะต้องกู้ข้อมูลที่เสียหายไป เนื่องจากการฟอร์แมตฮาร์ดดิสก์เราจะใช้โปรแกรม UNFORMAT กู้ข้อมูลกลับมา (แม้ว่าจะไม่มี IMAGE.DAT ก็สามารถใช้ UNFORMAT ได้ แต่ข้อควรระวังก็คือ ถ้าฮาร์ดดิสก์มีข้อมูลอยู่ ชื่อไฟล์ต่าง ๆ จะถูกทำลายหมด ถ้ามี IMAGE.DAT เราสามารถได้ชื่อไฟล์กลับมา แต่ข้อมูลที่เกิดหลังจากนั้นจะไม่สามารถกู้กลับมาได้ ยกเว้นแต่ใช้โปรแกรมอื่นเช่น DISKEDIT, UNERASE เข้าช่วย) การกู้ข้อมูลกลับมาก็ทำได้ โดยสั่ง UNFORMAT ซึ่งจะมีขั้นตอนตามรูปที่ 2-8

ขั้นแรก (รูปที่ 2) โปรแกรม UNFORMAT จะถามว่า จะทำการ UNFORMAT กับไดรฟ์ใด

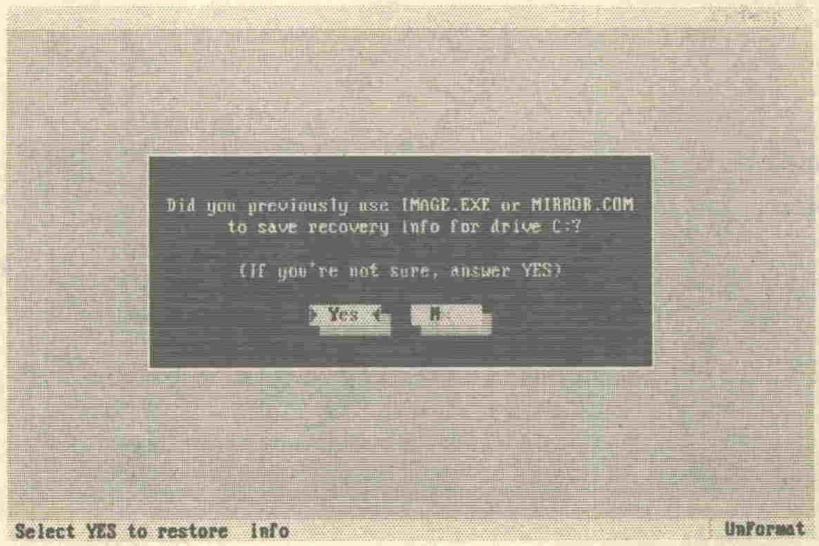
ขั้นที่ 2 (รูปที่ 3) โปรแกรม UNFORMAT จะถามว่า เราเคยใช้โปรแกรม IMAGE หรือ MIRROR (จะสามารถใช้ข้อมูลของ MIRROR ซึ่งเกิดจากการใช้ดอส 5.0 ได้เช่นเดียวกันกับ IMAGE.DAT) ถ้าเราเคยใช้ IMAGE, MIRROR หรือไม่แน่ใจว่า

```
C:\NORTON>image /?
Image, Norton Utilities 6.01, Copyright 1991 by Symantec Corporation

Saves disk system information for file and disk recovery.

IMAGE [drive:] [/NOBACKUP]

  drive         Save information for this drive.
  /NOBACKUP     Don't create a backup of the information file.

Image can be run in your AUTOEXEC.BAT file to save disk
information whenever you start your computer.  UnFormat
and UnErase make use of Image system files.

C:\NORTON>
```

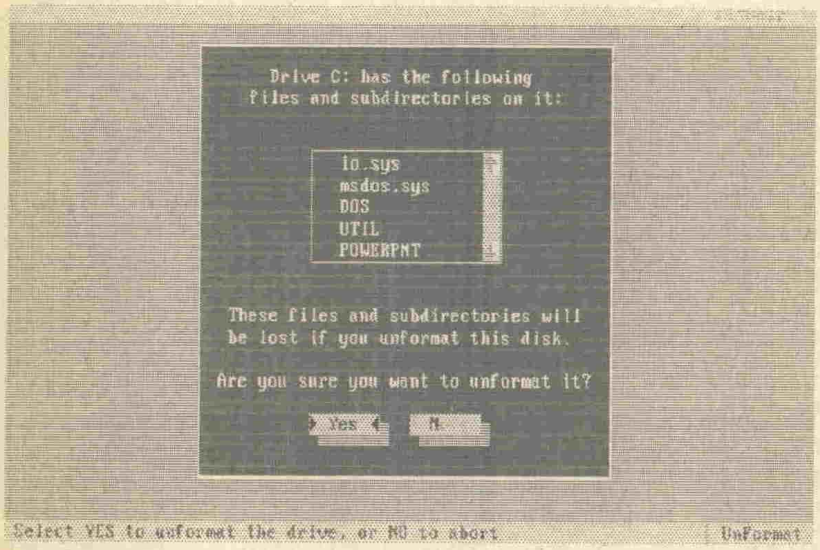
รูปที่ 1



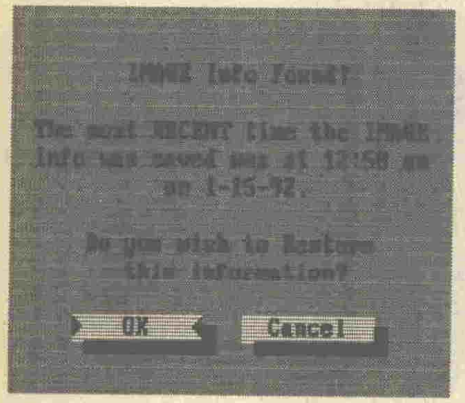
รูปที่ 2



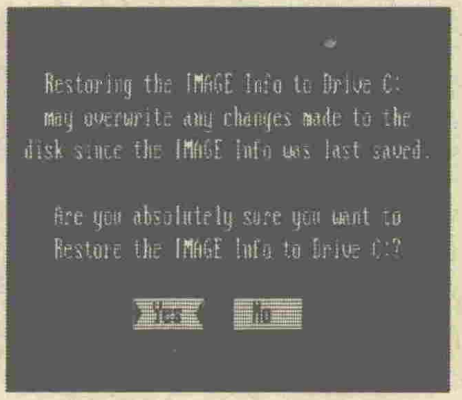
รูปที่ 3



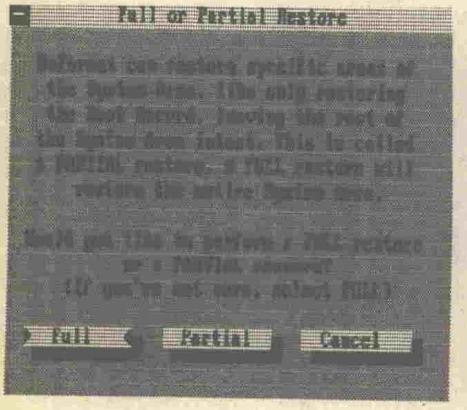
รูปที่ 4



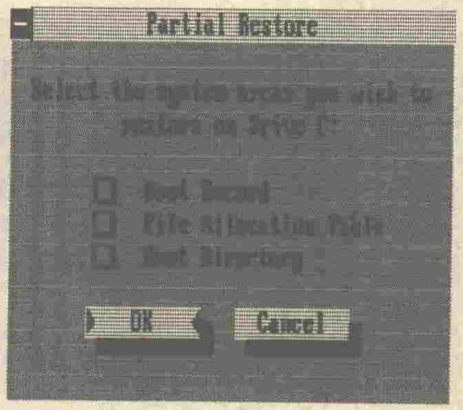
รูปที่ 5



รูปที่ 6



รูปที่ 7



รูปที่ 8

เคยใช้หรือไม่ ให้ตอบ Yes

ขั้นที่ 3 (รูปที่ 4) ในกรณีที่ฮาร์ดดิสก์ของเรามีข้อมูลอยู่ โปรแกรม UNFORMAT จะเตือนเราว่าชื่อไฟล์ของข้อมูลเหล่านั้นจะหายไป ถ้าไม่ต้องการทำ UNFORMAT ต่อให้เราตอบ No

ขั้นที่ 4 (รูปที่ 5) ในกรณีที่มี IMAGE.DAT โปรแกรมจะบอกว่าพบ IMAGE.DAT และจะบอกว่า IMAGE.DAT ครั้งล่าสุดเมื่อวันที่และเวลาเท่าไร เพราะถ้า IMAGE.DAT เป็นของวันที่ที่เก่าเกินไป จะทำให้ข้อมูลหลังจากวันที่ดังกล่าวไม่ถูกกู้กลับมา

ขั้นที่ 5 (รูปที่ 6) จะเป็นคำเตือนว่า ถ้าใช้ IMAGE.DAT ข้อมูลหลังจากวันที่ที่สร้าง IMAGE.DAT จะไม่ได้คืนกลับมา

ขั้นที่ 6 (รูปที่ 7) จะเป็นทางเลือกว่าจะ UNFORMAT ทั้งหมด คือ บูตเรคอร์ด, FAT และไดเรคทอรีเลยหรือไม่ ถ้าเลือกบางส่วนจะเป็นตามรูปที่ 8

สำหรับการทำ UNFORMAT จะมีขั้นตอนทั้งหมดดังด้านบน ก็ทำ UNFORMAT สามารถทำได้กับฮาร์ดดิสก์ที่ไม่ได้ทำอิมเมจไว้ได้เพราะการฟอร์แมตฮาร์ดดิสก์ของดอส ไม่ได้ทำการลบข้อมูลจริง ๆ ข้อมูลต่าง ๆ จึงอยู่กับฮาร์ดดิสก์เพียงแต่ FAT และไดเรคทอรีหายไป ยกเว้นดอสบางตัว เช่น Compaq DOS 3.1 และ AT&T DOS 2.11 จะทำลายข้อมูลของฮาร์ดดิสก์ทั้งหมด จึงไม่สามารถใช้ UNFORMAT มากู้สถานการณ์ได้ บทความนี้คงจบแค่นี้ แม้ว่า IMAGE ในที่นี้จะไม่เหมือน IMAGINE แต่ถ้าเราไม่ใช้ IMAGE เอาไว้ก่อน ฝันของเราอาจเป็นฝันร้ายก็ได้นะครับ